Protect Cloud-Native Applications at Runtime with Trend Micro Cloud One™ – Application Security

By Ian Heritage

Table of contents

Purpose of This Guide:

This Application Security user guide provides both DevSecOps teams and DevOps teams with an understanding of the importance of embedding runtime application security controls in the application build workflow to protect cloud-native web applications and APIs.

In addition, this guide outlines the value that Trend Micro Cloud One™ – Application Security brings to an organization's microservices architecture and the steps needed to get started with Trend Micro's deployment.

> "Almost 70% of web applications were vulnerable to breaches of sensitive data, with most of the data containing personal information or credentials."[2]
>
> - Jonathan Greig, TechRepublic

There is an Increased Focus on Web Application Attacks

There has been a notable surge in the use of web applications across all sectors of our changing economy and society. As businesses are relying on a wide range of applications for daily organizational processes and tasks, the general population has adapted to a new way of life across areas like retail, education, and entertainment to name a few.

However, web applications can introduce risks to those unsuspecting users and cause strain on the application development teams that build them. According to Verizon's 2020 Data Breach Investigations Report, the majority of breaches were caused by web application attacks, making it the top hacking vector amongst breaches.[1]

Web applications continue to be the main entry point in these attacks, and this trend seems to be here to stay for the foreseeable future. Further gaps in security will lure hackers to these targets as apps become a greater necessity for businesses and end users, and the data collected from these apps continues to be valuable.

The reality of web application attacks accounting for the majority of breaches demands a need for better protection and visibility. Applications that are not secured and monitored continually are a prime attack target for cybercriminals trying to disrupt organizations, typically for financial gain and corporate espionage.

[1] 2020 Data Breach Investigations Report, Verizon
[2] Report: 9 Times Out of 10, Hackers Can Attack Website Visitors, TechRepublic

Top Hacking Vectors in Breaches

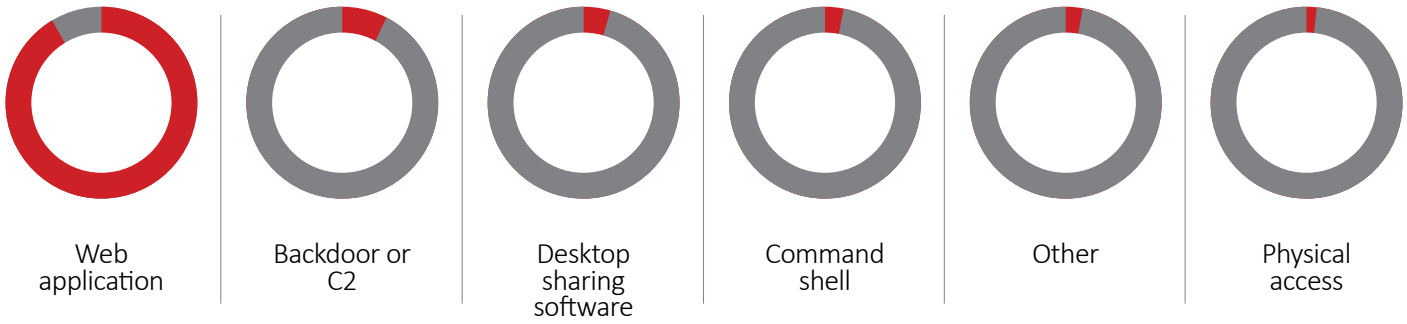


Figure 21

Top Hacking vectors in breaches (n=1,361)

Adoption of Cloud-Native Applications

With enterprises developing applications at lightning speed, technology trends have shifted from traditional monolithic web applications development to modern microservices and serverless architectures. This allows organizations to deliver applications and their updates at a more rapid and required pace.

This has increased the challenge for development and security teams to work together in order to ensure cloud-native applications are adequately protected from attacks. This is achieved through instilling a defence-in-depth strategy that crosses the continuous integration and continuous deployment methodology (CI/CD). Traditional security controls don't provide the security needed to protect cloud platforms. You need a modern, cloud-native instrumented system to gain the visibility needed for today's cloud-native threats.

> "Serverless is the fastest-growing cloud service model right now, with an annual growth rate of 75%."[3]
>
> - Christopher Null, TechBeacon

Top threats targeting applications commonly result in theft of credentials, sensitive data, and code. With these attacks now commonplace, organizations are looking to protect against the new attack surface. The increased use of cloud-native applications raises a new set of challenges due to the high rate of code changes and fast pace of development. This increases the potential to introduce software bugs and security vulnerabilities.

[3] The State of Serverless: 6 Trends to Watch, TechBeacon

Securing Your Cloud-Native Applications

Security processes can encompass the early stages of the cloud-native application life cycle. While developers are committing code and building container images, security protocols must be in place to identify open source, container image, and registry security gaps such as vulnerabilities and malware to help mitigate risks early and reduce costs. However, as applications remain vulnerable at runtime while they are deployed, security professionals must consider all avenues of threats and should not be complacent when it comes to securing the full application life cycle. From code changes that have not been tested but slip through to production, to zero-day attacks, runtime applications will continue to require examination.

Whether building applications on-premises, as a container in the cloud, or using serverless designs, security tools shouldn't interfere with the development pipeline nor the end to end visibility, monitoring, and detection is a top priority for security champions to manage.

Traditionally, organizations have protected their application using network protection tools ranging from network firewalls, intrusion prevention systems (IPSs), or web application firewalls (WAF). However, it has become a realization that these controls are limited to looking at the web traffic and lack the visibility into the running application.

While a WAF adds an extra layer of protection, today's attacks can bypass the WAF with automated tools. Additionally, maintaining a WAF requires a lot of heavy lifting. You need a team that can monitor its complexity, ensure proper configuration or adherence to rules, develop expressions, and input validation, which adds up to a lot of time and money on top of existing license costs.

Application security is deployed quickly and provides deep instrumentation and continuous detection and protection before cybercriminals can infiltrate the application. Organizations are shifting to runtime application security, which allows them to embed security controls directly into the application by default.

This facilitates the increasing speed of development and the ability to build applications that can be pushed to public cloud environments and services with the security controls built in. By helping protect your application immediately upon deployment, security teams can be assured that applications across modern platforms are going to be able to prevent threat actors from penetrating the application. This also allows development teams to gain better insight and remediation steps to identify security gaps at runtime.

Benefits of Application Security for CISOs and Security Champions

While Chief Information Security Officers (CISOs) and security champions may have different roles, they do have one fundamental goal; secure the business and protect data. However, with employees and customers working from home, and shifts in how business is delivered, continuous delivery models for applications now require security teams to think differently and address security threats more vigorously. This transition requires that security and development work closer together to plan and organize the protection of the enterprise and its data in a much more focused manner.

As a number organizations rely on IT departments to implement and manage their cybersecurity systems, many that have specific security teams are often only made up of a few specialists. These experts are tasked with managing multiple security tools across various parts of the business—from networks, cloud platforms, development workflows, and endpoints—all while spending considerable time responding to potential threats. In order to minimize this complex responsibility across a broad environment, security must be automated and efficient so that it works with the team and not against it. The CISO must implement a detection and protection system that reduces the burden on security teams. This can be applied by reducing the number of tools, and implementing a more focused security strategy that can reach all areas of the business with the right capabilities. This is important to help reduce security distractions and mitigate stress that can come between security teams and business units.

So, what should security professionals consider when looking at their Application Security posture? With the adoption of DevOps practices, CISOs and security champions need to be constantly assessing their state of application security to be sure it is meeting the pace of change across development teams. Security must integrate into DevOps workflows for better development and security collaboration and remediation across traditional and cloud-native application architectures.

CISO

With cloud-native applications changing rapidly, CISOs need to ensure their security program evolves to address the security challenges surrounding these rapidly changing applications

Security strategies now need evolved policies and standards for cloud-native application security testing and remediation.

It is important to have thorough build pipeline protection, policy compliance, and audibility that can be embedded in the fast, iterative CI/CD and DevOps processes.

Building a security culture where security champions are embedded into application development must come from the top, as this is key to empowering teams to follow processes and policies early on in building secure applications.

Security Champions

With each application bringing new risks and a new attack surface for potential exploitation, security champions will act as safety advocates across teams to ensure exceptions are caught fast and remediated quickly.

With the shifting mindset of security vs. developers to one that truly embraces integration, security will be an embedded function of safe application delivery.

Working with security policies and standards that have been defined, these will need to be automated, being applied consistently and quickly as part of the development process.

This automation will allow security teams to focus on exceptions which require a more focused skillset.

The Right Place for Modern Application Security

Public container images can have a significant number of vulnerabilities unbeknownst to the developer that uses them for application requirements. Identifying application security risks is not a top-of-mind task and can begin to erode the organization's build cycle and cloud environment, leading to application downtime and technical liabilities. To highlight this, a recent Snyk study indicated that, "35% of vulnerabilities were fixed in under 20 days", but "36% took 70 days or more to be remediated". As this can lead to possible breaches, fixing those bugs in the early development phase of software could reduce the information security risks facing many organizations today.

To do that, a number of technologies are available to help developers catch security flaws before they're baked into a final software release.

[4] State of Open Source Security Report 2020, Snyk

SAST

SAST has difficulties scanning and reporting on cloud-native applications because static tools only see the application source code it can follow. As more cloud-native apps are now developed with libraries and third-party components, this generates failures in the tool processing these links.

DAST

DAST interactively testing the applications from the outside requires the application to be fully built upon every code change. As DAST requires the application to be fully built upon every code change, this prevents the application from fitting well into an agile CI/CD pipeline. It also only provides an external view of security, while forgoing what's happening inside the application.

Both SAST and DAST are older technologies which provide less effective security for cloud-native applications and can impede on faster agile deployment strategies where DevOps teams require security tools to keep up with the pace of development.

IAST

IAST is an evolution to combine the benefits of both SAST and DAST with a developer-friendly approach. It is designed to work with development, testing, and/or QA environments to identify security vulnerabilities inside the application. In addition, it can be used in production environments to test traffic rapidly. This instant feedback can then be easily used to remediate via automation, or back to the developer, for code changes—typically actioned in the next application build.

However, there is an urgent need to implement modern security that will protect production applications from malicious and unforeseen threats in real time. Through deep instrumentation, application security must be able to detect weaknesses and vulnerabilities across today's modern code streams—as well as platforms like APIs, containers, and serverless applications—without deploying numerous tools and relying on multiple skill sets.

Application security must also bring greater value to both security champions and application engineers by deploying security that can improve the pace of remediation and response. This allows organizations to monitor traffic and block attacks in real-time.

A New Type of Application Security is Needed: "RASP"

Gartner defines runtime application self-protection (RASP) as, "a security technology that is built or linked into an application or application runtime environment and is capable of controlling application execution and detecting and preventing real-time attacks".[5]

RASP provides a level of visibility and detection that network security controls cannot achieve by operating within the context of the application. Instead of monitoring the application for potentially malicious inputs, RASP only processes inputs that could change the behavior or operation of the application.

RASP has two modes:

1. **In *detect mode*, the software monitors calls to the application and sounds an alarm if a suspect call is made.**
2. **In *mitigate mode*, RASP can prevent the execution of suspect instructions or terminate a user session.**

This approach has the potential to increase accuracy without significantly impacting the performance of the application.

Benefits of RASP

- **Security is provided anywhere you choose to place your application**
- **Embedded via code so doesn't slow down development**
- **Offers real-time protection and insight at runtime**
- **Vulnerability coverage is comprehensive and automatic**
- **Works at scale and tailored for scaling applications**
- **Provides insight into the application behavior that perimeter security lacks**

[5] Information Technology: Gartner Glossary, Gartner

Introducing Trend Micro Cloud One – Application Security

Trend Micro Cloud One – Application Security is an evolution in protection, providing real-time application security-as-a-service. Delivered as part of its industry-leading Trend Micro SaaS platform, Application Security provides code-level visibility and protection against the latest cyber threats from the inside.

Increase confidence in your web application security, quickly and easily build protection into your application. With just two lines of code, your applications will be secure, helping to minimize your risk and deliver greater visibility into the safety of your applications.

Application Security reduces the need for multiple application security tools across old and new platforms as well as coding languages. This security provides active guardrails and runs as a passive background process that doesn't interfere with your release pipeline and schedule.

Once deployed, Applications Security notifies your security and operations teams according to pre-configured policies and provides them with highly accurate attack forensics to facilitate an effective response.

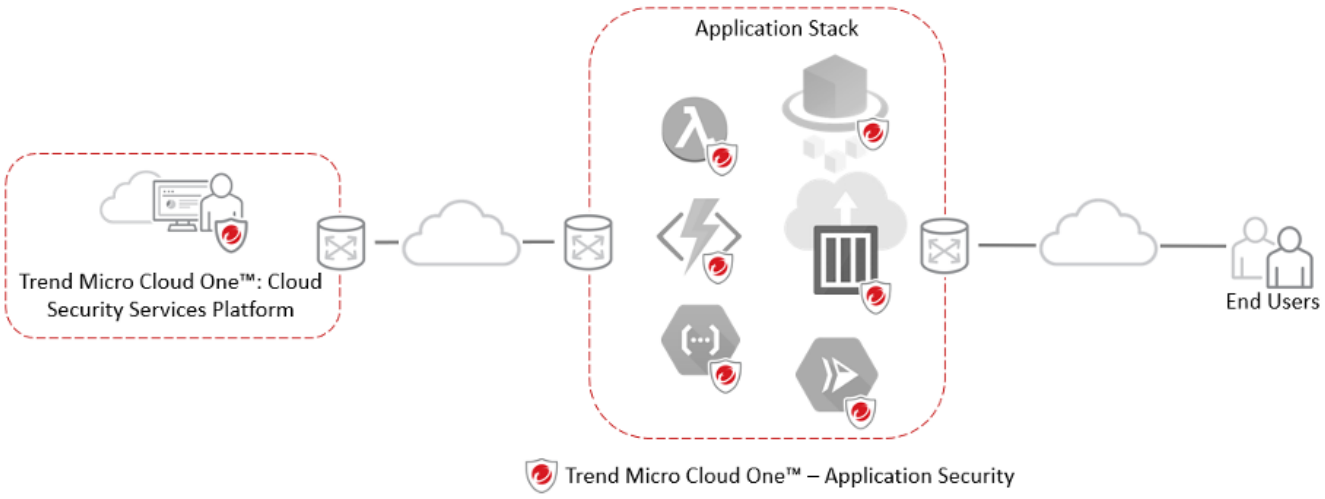
In addition, Application Security guards against determined attackers who are continuously running scanners against your application, creating malicious user accounts, fuzzing various elements, triggering exceptions, and attempting to run exploitation tools.


Use broad platform support to maintain your legacy applications and security for modern architectures. This including containers and serverless compute environments
Detect and block vulnerabilities and malware automatically at runtime
Utilize protection that is difficult to evade or bypass
Application Security allows you to:
Gain visibility into application threats with detailed forensics that investigate right down to the line of code
Use broad language support for traditional application designs, as well as cloud-native architectures
Install IPS rules for vulnerabilities in web applications
Analyze the execution of the app
Manage centralized visibility and control with Trend Micro Cloud One™ management

Trend Micro Cloud One Secures Your Applications at Runtime

Imagine having time in your day to focus on other security and operations tasks without the constant monitoring of your organization's applications sprawled across departments and development teams?

By embedding Application Security in your applications, you will receive alerts as soon as attackers begin conducting scans and attacks. You won't just have the ability to stop runtime attacks before they occur, but the capability for developers to pinpoint vulnerabilities in their code that the attack could exploit.



Whether applications are developed in-house or by a third parties, code identification helps DevOps and security operations teams prioritize their response and take effective next steps to resolve security issues. Using the Trend Micro Cloud One platform, teams can implement a range of security services and compliance checks alongside Application Security without hindering agile cloud development and deployment processes.

Application Security 101 outlines the top-most common risks to applications that software developers should be mindful when securing code. The Open Web Application Security Project (OWASP) foundation has a comprehensive list of risks of web applications and APIs. While Application Security protects against all OWASP listed risks, it is important that developers are aware of the most common application security risks:

Insufficient logging and monitoring

Lack of capability in detecting threats could allow malicious actors to tamper, extract, or destroy data, as well as further attack systems, maintain persistence, and pivot to more systems.

Injections

Flaws in or improper configuration of SQL, NoSQL, OS, and LDAP can be abused in injection attacks. For example, untrusted data may be sent to a code interpreter through a form input or other data submission methods to a web application. This could lead threat actors to use hostile data to trick the interpreter into executing malicious commands or providing unauthorized data access.

Data leaks and exposure

Web applications that do not properly protect sensitive data could allow threat actors to steal or modify weakly protected data. They could also conduct malicious activities such as credit card fraud and identity theft, among others. Improperly configured or badly coded APIs could also lead to a data breach.

You can address each event manually or you can configure Application Security to react automatically to attackers, stopping them in their tracks before any damage is done.

Most importantly, real vulnerabilities are not exploited because of the runtime protection, and your developers will have code-level information regarding the vulnerability that they have an immediate feedback loop to fix. Application Security helps you accelerate time-to-market for the software without compromising security.

Requirements to Get Started

Setup is simple. All you need is a Trend Micro Cloud One account, with Application Security enabled.

Sign up for the free trial now and get access to the entire Trend Micro Cloud One service platform.

How to Get Started with Deployment

Install the Trend Micro Cloud One – Application Security Agent

Follow the simple steps here to deploy a new agent into your application.

a. Integrating an agent into your application depend on your supported framework. The supported platforms are:

i. **Python**

ii. **Node.js with Express**

iii. **PHP**

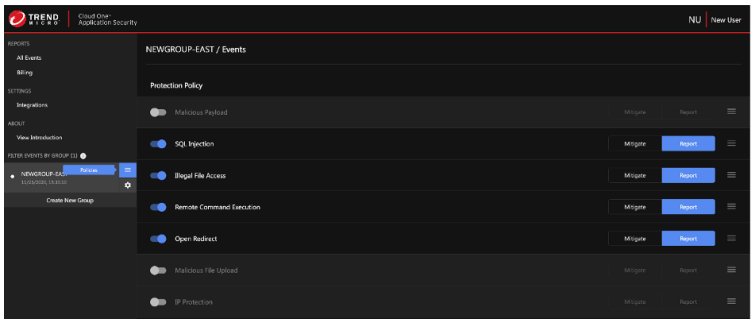
iv. **Java**

v. **.NET**

We will continue to add new frameworks to our supported list based on market demand.

1. Define security policy

The runtime security policy identifies the rules and procedures to secure your application.



---

2. Embed micro-agent into code

The runtime security policy identifies the rules and procedures to secure your application.

```
Starting agent-java v3.3.1...
Agent is ready
```

---

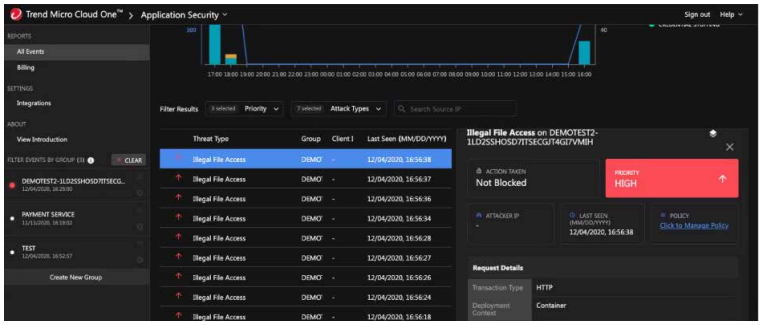
3. Deploy app

The agent will discover the make-up of the cloud-native application, enabling it to automatically defend your organization.

---

4. Protect and monitor the app

Application Security acts automatically and notifies the security teams according to pre-configured rules with specific attack forensics.



Why Trend Micro for Your Web Application Security?

Securing web applications has become paramount in defense-in-depth security strategies. Understanding risks and vulnerabilities in an organization's applications inventory is a huge undertaking and to achieve success, security must be treated as a fundamental part of the CI/CD process. End users of an organization's applications whether internal employees or external customers have an expectation that DevOps practices will deploy updates to applications securely, while limiting regression and performance lags in runtime. However, end users seldom consider the depth of security implementation or chances of vulnerabilities affecting their business.

Application Security brings insight and direct runtime responses to web application attacks and vulnerabilities, delivering broad threat detection and protection from within the application. The ability to quickly deploy and detect runtime threats, prevent zero-day attacks, and stop threat actors gives development teams a distinct view into security bugs. In addition, it provides security teams with the benefit of introducing application security as part of the build pipeline without having to introduce larger security interruptions.

Trend Micro helps facilitate the collaboration between development teams and security teams. But more importantly, Trend Micro supports developers to do the right thing. Trend Micro has the breadth of choice in how organizations want to get started or expand in the cloud. Cloud Security doesn't just mean securing a workload, there are multiple vectors from the build

pipeline code and components, policy configuration, container deployment (including Kubernetes®), and runtime protection. This also includes being prepared to secure new services offered by cloud providers that compliment or add value to application designs and workflows, such as object storage services. In addition, customers need the choice of a broad platform support for their security investment across their hybrid cloud and growing cloud initiatives.

Trend Micro helps to make the world safe for exchanging digital information today and in the future. This is done by delivering complete coverage for your modern and evolving hybrid and multi-cloud workload and application security requirements—from build time to runtime.

Backed by 24/7 global threat research and extensive support, you can enjoy peace of mind as you design and expand your hybrid and multi-cloud application footprint. We help security teams reduce the constraints on development teams and the operational complexities associated with the growing threat landscape by enabling better and faster protection that is integrated into your entire application life cycle.

For more information, please visit our Trend Micro Cloud One – Application Security page.

TREND MICRO™ Securing Your Connected World

[UG00_Application_Security_User_Guide_210202US]